(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平5－250326

(43)公開日　平成５年(1993)９月28日

(51)Int.Cl.[5]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ	15/00	３３０	Ｇ　7459－5Ｌ		
	15/21	３４０	Ｃ　7218－5Ｌ		
Ｇ０６Ｋ	17/00		Ｄ　7459－5Ｌ		
			Ｔ　7459－5Ｌ		

審査請求　未請求　請求項の数15(全 23 頁)

(21)出願番号　特願平4－49830

(22)出願日　平成４年(1992)３月６日

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号

(72)発明者　大野　久支
伊丹市瑞原４丁目１番地　三菱電機株式会社北伊丹製作所内

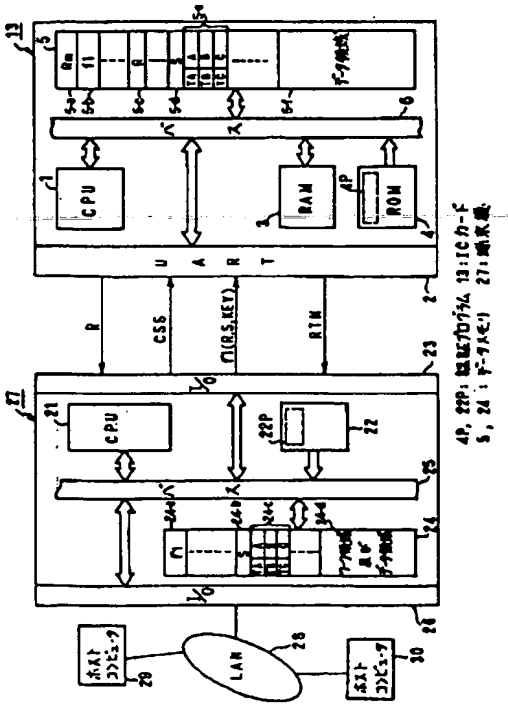
(74)代理人　弁理士　曾我　道照　（外６名）

(54)【発明の名称】　ＩＣカードと端末機との間の認証方法およびそのシステム

(57)【要約】

【目的】　ＩＣカードと端末機との間での認証を、認証コード或はこれのアドレスを直接、双方の間で伝送することなく行うことにより、セキュリティの高い認証方法を得ることを目的とする。

【構成】　それぞれ対応する時間情報を有する複数の認証コード、および暗号化アルゴリズムをＩＣカードおよび端末機の双方がそれぞれ格納しており、ＩＣカードおよび端末機の一方で１つの認証コードを選択してこれを暗号化アルゴリズムで暗号化して認証データとして他方へ送ると共に、コマンド間或は信号間の時間を利用して選択された認証コードに対応する時間情報を他方へ送る。他方では、送られた時間情報から割り出された認証コードを同様に暗号化アルゴリズムにより暗号化して認証データを発生し、他方からの認証データと比較する。



1

【特許請求の範囲】

【請求項１】　ＩＣカードおよび端末機がそれぞれ、対応する時間情報をそれぞれ有する複数の認証コード、所定のアルゴリズムに従ってデータを暗号化する暗号化手段、およびタイマ手段を有し、上記ＩＣカードおよび端末機の一方がさらに乱数を発生する手段および比較手段を有する上記ＩＣカードおよび端末機の間で認証を行う、ＩＣカードと端末機との間の認証方法であって、

ＩＣカードおよび端末機の上記一方の装置で乱数を発生し他方へ送信する工程と、

上記他方の装置において、受信した乱数を上記複数の認証コードのうちの１つの認証コードをキーとして上記アルゴリズムに従って暗号化して認証データを発生する第１暗号化工程と、

上記他方の装置において、所定の信号が送信された後、使用した上記認証コードに対応する時間情報の時間が経過後に上記暗号化された認証データを一方の装置に送信する工程と、

上記一方の装置において、上記所定の信号が送信された後、上記他方の装置から認証データを受けるまでの間の時間間隔をカウントし、カウントされた時間間隔と一致する時間情報に対応する認証コードをキーとして、上記乱数を上記他方の装置と同様に上記アルゴリズムに従って暗号化して認証データを発生する第２暗号化工程と、

上記一方の装置において、上記第２暗号化工程で作られた認証データと、上記他方の装置から送信された認証データとを比較して、一致したか否かを示す結果信号を上記他方の装置へ送信する工程と、

を備えたＩＣカードと端末機との間の認証方法。

【請求項２】　上記ＩＣカードおよび端末機のうちの上記他方の装置が上記乱数受信後にカウント開始信号を上記一方の装置に送信する工程をさらに含み、上記認証データ送信工程では、上記カウント開始信号送信後、使用した上記認証コードに対応する時間情報の時間が経過した後に上記認証データが一方の装置に送信され、上記第２暗号化工程では、上記一方の装置で上記カウント開始信号を受信した時から上記認証データを受信するまでの間の時間間隔をカウントし、カウントされた時間間隔と一致する時間情報に対応する認証コードをキーとして、上記乱数を上記他方の装置と同様に暗号化する請求項１のＩＣカードと端末機との間の認証方法。

【請求項３】　上記認証データ送信工程では、上記ＩＣカードおよび端末機のうちの上記他方の装置において上記乱数を受信後、使用した上記認証コードに対応する時間情報の時間が経過した後に上記認証データが一方の装置に送信され、上記第２暗号化工程では、上記一方の装置において上記乱数を送信した時から上記認証データを受けた時までの間の時間間隔をカウントし、カウントされた時間間隔と一致する時間情報に対応する認証コードをキーとして、上記乱数を上記他方の装置と同様に暗号

2

化する請求項１のＩＣカードと端末機との間の認証方法。

【請求項４】　上記ＩＣカードが上記アルゴリズムを予め格納していない場合に、上記認証作業の乱数送信工程の前に、上記暗号化用のアルゴリズムを上記端末機からＩＣカードへロードするアルゴリズムロード工程をさらに含む請求項１のＩＣカードと端末機との間の認証方法。

【請求項５】　上記第１暗号化工程において、ＩＣカードと端末機の間のトランザクションの回数をカウントし、所定の値に達した時に選択する認証コードを変える請求項１のＩＣカードと端末機との間の認証方法。

【請求項６】　上記ＩＣカードおよび端末機がそれぞれＮ個の認証コードを有し、上記第１暗号化工程において、上記乱数をＮで割り、余りをｍとすると、ｍ＋１番目の認証コードを選択するようにした請求項１のＩＣカードと端末機との間の認証方法。

【請求項７】　ＩＣカードと端末機とがそれぞれ、対応する識別子をそれぞれ有する複数の認証コード、複数のアルゴリズム、これらのアルゴリズムに従ってデータの暗号化を行う暗号化手段をそれぞれ有し、上記ＩＣカードと端末機の一方がさらに乱数を発生する手段、複合化手段および比較手段を有する上記ＩＣカードおよび端末機の間で認証を行う、ＩＣカードと端末機との間の認証方法であって、

ＩＣカードおよび端末機の上記一方の装置で乱数を発生し他方へ送信する工程と、

上記他方の装置において、受信した乱数を上記複数の認証コードのうちの１つの認証コードをキーとして第１のアルゴリズムに従って暗号化して認証データを発生すると共に、第２のアルゴリズムに従って上記認証コードの識別子を暗号化する第１暗号化工程と、

この第１暗号化工程で作られた暗号化されたデータをそれぞれ上記一方の装置に送信する工程と、

上記一方の装置において上記識別子を暗号化したデータを複合化して対応する認証コードを得るための複合化工程と、

この複合化工程で得られた認証コードをキーとして、上記乱数を上記他方の装置と同様に第１のアルゴリズムに従って暗号化して認証データを発生する第２暗号化工程と、

この第２暗号化工程で生成された認証データと、上記他方の装置から送信された認証データとを比較して、一致したか否かを示す結果信号を他方の装置へ送信する工程と、

を備えたＩＣカードと端末機との間の認証方法。

【請求項８】　双方の間の認証作業を行うＩＣカードおよび端末機からなるシステムであって、

上記ＩＣカードおよび端末機がそれぞれ、

少なくとも１つの暗号化用のアルゴリズム、少なくとも

１つのシステムキー、それぞれ対応する時間情報を有する複数の認証コード、および認証作業を行うための認証プログラムを含むプログラムを格納した記憶手段と、
データの入出力制御を行う入出力制御手段と、
上記記憶手段に格納されたプログラムに従ってデータの処理および制御を行うと共に、上記認証プログラムに従って認証作業を行うデータ制御・処理手段と、
時間をカウントするタイマ手段と、
上記各手段を接続するバス手段と、を備え、上記ＩＣカードおよび端末機の一方の装置がさらに、上記認証プログラムに従って上記データ制御・処理手段の制御によりそれぞれ行われる、
乱数を発生して他方の装置に送信する手段と、
所定の信号が送信された時から、上記他方の装置からの暗号化された認証データを受けた時までの間の時間間隔を上記タイマ手段によりカウントし、カウントされた時間間隔と一致する時間情報に対応する認証コードをキーとして、上記乱数を上記他方の装置と同様に上記アルゴリズムに従って暗号化して認証データを発生する暗号化手段と、
この暗号化手段で作られた認証データと上記他方の装置から送信された認証データとを比較して、上記他方の装置へ一致したか否かを示す結果信号を送信する手段と、
を備え、上記ＩＣカードおよび端末機の他方の装置がさらに、上記認証プログラムに従って上記データ制御・処理手段の制御によりそれぞれ行われる、
上記一方の装置から受けた乱数を上記複数の認証コードのうちの１つの認証コードをキーとして上記アルゴリズムに従って暗号化して認証データを発生する暗号化手段と、
この暗号化手段で作られた認証データを、上記所定の信号が送信された時から、使用した上記認証コードに対応する時間情報の時間が経過後に上記一方の装置に送信する手段と、
を備えたＩＣカードおよび端末機からなるシステム。

【請求項９】　上記カウントの基準となる上記所定の信号が上記一方の装置から他方の装置に送信される上記乱数である請求項８のＩＣカードおよび端末機からなるシステム。

【請求項１０】　上記ＩＣカードおよび端末機の上記他方の装置が、上記一方の装置に対してカウント開始信号を送信する手段を有し、上記カウントの基準となる上記所定の信号が上記カウント開始信号である請求項８のＩＣカードおよび端末機からなるシステム。

【請求項１１】　上記ＩＣカードが上記アルゴリズムを予め格納していない場合に、上記端末機が、上記アルゴリズムを上記ＩＣカードへロードするアルゴリズムロード手段をさらに含む請求項８のＩＣカードおよび端末機からなるシステム。

【請求項１２】　上記他方の装置が、ＩＣカードと端末機の間のトランザクションの回数をカウントし、所定の値に達した時に選択する認証コードを変える認証コード選択手段をさらに備えた請求項８のＩＣカードおよび端末機からなるシステム。

【請求項１３】　上記ＩＣカードおよび端末機がそれぞれＮ個の認証コードを有し、上記他方の装置が、上記乱数をＮで割り、余りをｍとすると、ｍ＋１番目の認証コードを選択する認証コード選択手段をさらに備えた請求項８のＩＣカードおよび端末機からなるシステム。

【請求項１４】　双方の間の認証作業を行うＩＣカードおよび端末機からなるシステムであって、
上記ＩＣカードおよび端末機がそれぞれ、
複数の暗号化用のアルゴリズム、複数のシステムキー、それぞれ対応する識別子を有する複数の認証コード、および認証作業を行うための認証プログラムを含むプログラムを格納した記憶手段と、
データの入出力制御を行う入出力制御手段と、
上記記憶手段に格納されたプログラムに従ってデータの処理および制御を行うと共に、上記認証プログラムに従って認証作業を行うデータ制御・処理手段と、
上記各手段を接続するバス手段と、を備え、上記ＩＣカードおよび端末機の一方の装置がさらに、上記認証プログラムに従って上記データ制御・処理手段の制御によりそれぞれ行われる、
乱数を発生して他方の装置に送信する手段と、
上記他方の装置から送信される上記識別子を暗号化したデータを複合化して対応する認証コードを得る識別子複合化手段と、
この識別子複合化手段で得られた認証コードをキーとして、上記乱数を上記他方の装置と同様に第１のアルゴリズムに従って暗号化して認証コードを発生する暗号化手段と、
この暗号化手段で作られた認証データと、上記他方の装置から送信された第１のアルゴリズムにより暗号化された認証データとを比較して、一致したか否かを示す結果信号を上記他方の装置へ送信する手段と、を備え、
上記ＩＣカードおよび端末機の他方の装置がさらに、上記認証プログラムに従って上記データ制御・処理手段の制御によりそれぞれ行われる、
上記一方の装置から受けた乱数を上記複数の認証コードのうちの１つの認証コードをキーとして第１のアルゴリズムに従って暗号化して認証データを発生すると共に、第２のアルゴリズムに従って上記認証コードの識別子を暗号化する暗号化手段と、
この暗号化手段で作られた暗号化されたデータをそれぞれ上記一方の装置に送信する手段と、
を備えたＩＣカードおよび端末機からなるシステム。

【請求項１５】　２つの電気的装置が、対応する時間情報をそれぞれ有する複数の認証コード、所定のアルゴリズムに従ってデータを暗号化する暗号化手段、およびタ

イマ手段をそれぞれ有し、両者の一方がさらに乱数を発生する手段および比較手段を有する、２つの電気的装置間で認証を行う認証方法であって、
上記２つの装置の上記一方の装置で乱数を発生し他方へ送信する工程と、
上記他方の装置において、受信した乱数を上記複数の認証コードのうちの１つの認証コードをキーとして上記アルゴリズムに従って暗号化して認証データを発生する第１暗号化工程と、
上記他方の装置において、所定の信号が送信された後、使用した上記認証コードに対応する時間情報の時間が経過後に上記認証データを一方の装置に送信する工程と、
上記一方の装置において、上記所定の信号が送信された後、上記他方の装置から認証データを受けるまでの間の時間間隔をカウントし、カウントされた時間間隔と一致する時間情報に対応する認証コードをキーとして、上記乱数を上記他方の装置と同様に上記アルゴリズムに従って暗号化して認証コードを発生する第２暗号化工程と、
上記一方の装置において、上記第２暗号化工程で作られた認証データと、上記他方の装置から送信された認証データとを比較して、一致したか否かを示す結果信号を上記他方の装置へ送信する工程と、
を備えた２つの電気的装置の間の認証方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】この発明は、ＩＣカードと端末機との間の認証方法およびそのシステムに関する。

【０００２】

【従来の技術】ＩＣカードと端末機との間の認証方法の従来技術として、例えば特開昭５９－７７５７５号公報(特公平３－４０８７９号公報)に開示されているものがある。この従来技術で示されている認証方法は、まず端末機側で乱数を発生させ、この乱数とカードに記憶されている目的の認証コードを特定するためのアドレスをカード側に送る。ＩＣカード側では与えられたアドレスより該当する認証コードを割り出す。そしてＩＣカード自身が持っている暗号器を使用して、与えられた乱数と割り出された認証コードを使って所定の処理を行い処理結果を導き出し、この結果を端末機側に送信する。端末機も認証コードに関する情報および暗号器をＩＣカードと同様に備えており、これを使用して乱数と認証コードからＩＣカードと同様の処理を行う。そしてこの処理結果とＩＣカードから送られて来た処理結果が一致すれば、該ＩＣカードを正当なものであると判断している。

【０００３】

【発明が解決しようとする課題】従来のＩＣカードと端末機との間の認証は以上のように行われていたが、目的の認証コードを得るために、端末機からＩＣカードへ認証コードが格納されている番地を示すアドレスを直接的に与えているために、不正使用者に認証コードが格納されている場所および内容を知られてしまう危険性があるという問題点があった。

【０００４】この発明は上記のような問題点を解消するためになされたもので、不正使用者にＩＣカード内の認証コードが格納されている番地(アドレス)およびその内容が知られることのない認証方法およびそのシステムを得ることを目的とする。

【０００５】

【課題を解決するための手段】上記の目的に鑑み、この発明は、ＩＣカードおよび端末機がそれぞれ、対応する時間情報をそれぞれ有する複数の認証コード、所定のアルゴリズムに従ってデータを暗号化する暗号化手段、およびタイマ手段を有し、上記ＩＣカードおよび端末機の一方がさらに乱数を発生する手段および比較手段を有する上記ＩＣカードおよび端末機の間で認証を行う、ＩＣカードと端末機との間の認証方法であって、ＩＣカードおよび端末機の上記一方の装置で乱数を発生し他方へ送信する工程と、上記他方の装置において、受信した乱数を上記複数の認証コードのうちの１つの認証コードをキーとして上記アルゴリズムに従って暗号化して認証データを発生する第１暗号化工程と、上記他方の装置において、所定の信号が送信された後、使用した上記認証コードに対応する時間情報の時間が経過後に上記暗号化された認証データを一方の装置に送信する工程と、上記一方の装置において、上記所定の信号が送信された後、上記他方の装置から認証データを受けるまでの間の時間間隔をカウントし、カウントされた時間間隔と一致する時間情報に対応する認証コードをキーとして、上記乱数を上記他方の装置と同様に上記アルゴリズムに従って暗号化して認証データを発生する第２暗号化工程と、上記一方の装置において、上記第２暗号化工程で作られた認証データと、上記他方の装置から送信された認証データとを比較して、一致したか否かを示す結果信号を上記他方の装置へ送信する工程と、を備えたＩＣカードと端末機との間の認証方法にある。

【０００６】また、この発明の別の実施例では、複数の認証コードに時間情報の代わりに識別子をそれぞれ割り当て、この識別子を暗号化して送り、受けた側ではこれを複合化して求められた識別子から選択された認証コードを割り出し、この認証コードをキーとして乱数を暗号化して認証データを発生し、送られてきた認証データと比較して認証を行う。また、この発明は上記認証方法を行うＩＣカードおよび端末機からなる装置としてのシステムも含む。

【０００７】

【作用】この発明に係る認証方法では、時間情報がそれぞれに割り当てられた複数の認証コードをＩＣカードと端末機とがそれぞれ設け、一方で選択された認証コードを相手側に伝える際には、該認証データの対応する時間情報をコマンドとコマンドの間の時間間隔として相手側

に伝達し、受けた側ではコマンド間の時間間隔から対応する認証コードを割り出す。そしてＩＣカードと端末機の双方で該認証コードをキーとして乱数を暗号化アルゴリズムに従って暗号化して認証データを発生し、これを比較して一致したことにより互いの正当性を確認する。

【０００８】また別の実施例では複数の認証コードにそれぞれ識別子を割り当て、一方で選択された認証コードを相手側に伝える際には、該認証データの対応する識別子を識別子暗号化用のアルゴリズムで暗号化して相手側に伝達し、受けた側ではこれを複合化して識別子を求めて認証コードを割り出す。そしてＩＣカードと端末機の双方で該認証コードをキーとして乱数を暗号化アルゴリズムに従って暗号化して認証データを発生し、これを比較して一致したことにより互いの正当性を確認する。

【０００９】これらの認証方法では認証コードおよびこれのアドレスを直接的に双方の間で送ることがなく、不正使用者に認証コードを知られることなく認証作業を行うことができる。

【００１０】

【実施例】以下、この発明の実施例を添付図面に基づいて説明する。図１はこの発明で使用されるＩＣカードの機能的構成の一例を示す。図において、ＩＣカード１３はＣＰＵ１、入出力制御回路(以下ＵＡＲＴ)２、ＲＡＭ３、ＲＯＭ４、データメモリ５、内部バス６を備えている。ＵＡＲＴ２はＩ／Ｏ端子７でのデータの入出力制御をする。ＲＡＭ３はＣＰＵ１で計算等に使用されるデータの一時記憶のためのメモリである。ＲＯＭ４はＣＰＵ１を駆動させるためのプログラムが格納される読み出し専用のメモリである。データメモリ５はこの発明では、認証コード(ＩＤコード)、認証コードテーブル、暗号化アルゴリズム、および一般的なデータ等を格納するためのメモリである。このデータメモリ５は通常、ＥＥＰＲＯＭからなる。内部バス６は上述した各機能ブロックを接続する。ＩＣカード１３はさらに電源端子８(Vcc)、クロック端子９(CLK)、リセット端子１０(RST)およびグランド端子１２(GND)を備えている。またタイマ回路１２はタイムカウントを専門に行う回路で、本願のＩＣカードはこれを内蔵する場合としない場合がある。

【００１１】このＩＣカード１３のハードウェアの構造は従来のものと何等変わりなく、データメモリ５が他の部分と一体になったワンチップ構造のものと、他の部分と分離されたマルチチップ構造のものとがある。動作は、カード外部からＩ／Ｏ端子７、ＵＡＲＴ２、バス６を介して命令が与えられると、この命令に基づいてＣＰＵ１がＲＯＭ４に格納されたプログラムに従って処理を行う。そしてその処理結果は、命令とは逆経路でカード外部へ出力される。この発明の認証作業(照合作業)についても同様に行われる。

【００１２】図２はこの発明の第１実施例で使用されるＩＣカードと端末機からなるシステムの機能的構成を示

すブロック図である。図２においてＩＣカード１３は図１に示したものである。ＩＣカード１３のデータメモリ５の内部には様々なデータが格納されている。領域５－ａには乱数発生アルゴリズム(Ｒｍ)、領域５－ｂには暗号化アルゴリズム(ｆ１)、領域５－ｃには乱数発生アルゴリズム(Ｒｍ)によって発生する乱数(Ｒ)、領域５－ｄには暗号化アルゴリズム(ｆ１)に使用されるシステムキー(Ｓ)、領域５－ｅには認証を行うための複数の認証コード(Ａ、Ｂ、Ｃ･･･)とこれらのそれぞれに割り当てられ時間情報(ＴＡ、ＴＢ、ＴＣ･･･)の関係を示すテーブルがそれぞれ格納されている。また領域５－ｆは一般のアプリケーション等に使用されるデータ領域である。認証コード(Ａ、Ｂ、Ｃ･･･)が格納された領域５－ｅの構成は図３に拡大して示した。テーブルはＴＩＭＥ７２およびＫＥＹ７３から構成されており、ＫＥＹ７３の個々の認証コード(Ａ、Ｂ、Ｃ･･･)には、ＴＩＭＥ７２の時間情報(ＴＡ、ＴＢ、ＴＣ･･･)がそれぞれ割り付けられている。そして認証コードをＫＥＹとして、対応する時間情報が割り出される。

【００１３】また図２において、端末機２７はＩＣカード１３との認証を行う端末機で、１つの端末機単独の場合もあれば、図示のように上位ホストコンピュータ２９、３０が接続されているＬＡＮ２８に接続されている場合もある。端末機２７の構成はＩＣカード１３とほぼ同様なものとなっており、バス２５を介してＣＰＵ２１ＲＯＭ２２、データおよびワーク領域のためのデータメモリ２４、入出力を制御するためのＩ／Ｏ(入出力制御回路)２３、２６が図示のように接続されている。データメモリ２４はＩＣカード１３のデータメモリ５と同様に様々はデータを格納している。領域２４－ａには暗号化アルゴリズム(ｆ' 1)、領域２４－ｂには暗号化アルゴリズム(ｆ' 1)に使用されるシステムキー(Ｓ)、領域２４－ｃには認証を行うための認証コード(Ａ、Ｂ、Ｃ･･･)がそれぞれ格納されている。また領域２４－ｄは、一般のアプリケーション等やＣＰＵ２１の一時記憶に使用されるワーク領域およびデータ領域である。認証コード(Ａ、Ｂ、Ｃ･･･)が格納された領域２４－ｃは図３に示したＩＣカード１３のデータメモリ５内の認証コードが格納された領域５－ｅと全く同じである。

【００１４】図４および図５には図２のシステムのＩＣカードと端末機との間で行われるこの発明の第１実施例による認証作業(動作)を説明するためのフローチャートを示した。図４はＩＣカード２７の動作のフローチャート、図５は端末機２７の動作のフローチャートである。これらの動作は、端末機２７およびＩＣカード１３のＣＰＵ２１、４により、それぞれのＲＯＭ２２、４に格納された認証作業用の認証プログラム２２Ｐ、４Ｐに従って行われる。

【００１５】以下に図２～図５に従ってこの発明の第１実施例の動作を説明する。この第１実施例における認証

方法を概略的に説明すると、まず、ＩＣカード１３側で乱数(R)を発生させてこれを端末機２７側へ送る。端末機２７側では認証の目的の認証コード(ＫＥＹ)と暗号化のためのシステムキー(S)を利用して暗号化アルゴリズム、例えば暗号化アルゴリズム(f' 1)の関数に基づいて暗号化された認証データf' 1(R、S、ＫＥＹ)を作り出し、ＩＣカード１３側へ認証のためのデータとして送り返す。なお、ここでの認証コード(ＫＥＹ)は必ずしも実際の認証コードそのものである必要はなく、図面ではＡ、Ｂ、Ｃ…として示した。ＩＣカード１３側は、ＩＣカード１３自身がデータメモリ５の領域５－ｅに格納している認証コード(ＫＥＹ)および、領域５－ｄに格納しているシステムキー(S)から端末機２７の暗号化アルゴリズム(f' 1)と同様の暗号化アルゴリズム(ｆ１)の関数に基づいて暗号化されたデータｆ１(R、S、ＫＥＹ)を同様に作り出し、送られてきた暗号化されたデータすなわち認証データf' 1(R、S、ＫＥＹ)と照合する。

【００１６】この第１実施例では、目的の認証コードを相手側に知らせる方法に工夫を凝らし、例えばアドレス等で直接的に知らせるのではなく、コマンドとコマンドの間の時間間隔を利用することにより、相手側に認証コードを知らせようというものである。

【００１７】図４および図５のフローチャートに従ってもう少し詳しく説明する。図４のフローチャートに示すように、ＩＣカード１３はデータメモリ５の領域５－ａに格納された乱数発生アルゴリズム(Ｒｍ)に従って乱数(R)を発生させ(ステップ４２)、端末機２７へ送信する(ステップ４３)。端末機２７は図５のフローチャートに示すように、乱数(R)を受信後(ステップ６２)、１つの認証コード(ＫＥＹ)を選択して認証データf' 1(R、S、ＫＥＹ)を作り出す(ステップ６３)。そしてさらにデータメモリ２４の領域２４－ｃに格納されたタイムテーブル(図３参照)から選択した認証コード(ＫＥＹ)(Ａ、Ｂ、Ｃ…のいずれか)７３の対応する時間情報(ＴＡ、ＴＢ、ＴＣ‥のいずれか)７２を割り出す。例えば、認証コードＢを選択した場合には、その時間情報はＴＢというぐわいに割り出す(ステップ６４)。

【００１８】そして端末機２７とＩＣカード１３の時間の同期を図るために、端末機２７はＩＣカード１３へカウント開始信号ＣＳＳを送信し(ステップ６５)、端末機２７側のカウンタをリセットする(カウントを０にする)(ステップ６６)。端末機２７およびＩＣカード１３は同期のためのカウンタとして、専用のハードウェアとしてのタイマ回路１２(図１参照)をそれぞれ備えていてもいいし、あるいはＣＰＵのソフトウェア上で行うカウンタ(特に図示せず)を使用してもよい。この第１実施例では、ＣＰＵのソフトウェア上で行うカウンタを使用したものとする。

【００１９】ＩＣカード１３もカウント開始信号(ＣＳＳ)を受信後(ステップ４４)、ＩＣカード１３側のカウンタをリセットし(カウントを０にする)(ステップ４５)、これにより端末機２７とＩＣカード１３との時間的同期を図る。端末機２７はカウント開始信号(ＣＳＳ)を送信してた後、タイムテーブルで設定されている時間情報の時間まで待ち(ステップ６７、６８、６９)、ＩＣカード１３へ認証データf' 1(R、S、ＫＥＹ)を送信する(ステップ７０)。ＩＣカード１３はカウント開始信号(ＣＳＳ)受信から認証データf' 1(R、S、ＫＥＹ)を受信するまでの時間をカウントし(ステップ４６、４７、４８)、そのカウントした値からデータメモリ５の領域５－ｅに格納されたタイムテーブルに基づいて選択された認証コード、すなわち認証するための認証コードを割り出す(ステップ４９、５０、５１、５２、５３、５４)。

【００２０】そして該当する認証コード(ＫＥＹ)より暗号化された認証データｆ１(R、S、ＫＥＹ)を算出し(ステップ５５)、端末機２７より送信された認証データf' 1(R、S、ＫＥＹ)との照合を行う(ステップ５６、５７、５８)。そして照合の結果、双方の認証データが一致したか否かを示す結果信号(ＲＴＮ)を端末機２７へ送信する(ステップ５９)。このようにすれば、直接的に認証コードが格納されているアドレスを端末機２７とＩＣカード１３間で送信することなく認証作業が行え、認証コードが格納されたアドレスを知られることなく、より安全に認証作業が行える。

【００２１】上記第１実施例では時間のカウントをＣＰＵのソフトウェア上で行っていたが、ＩＣカードおよび端末機がそれぞれ専用のタイマ回路(図１の符号１２参照)を備えていてもよい。この場合、タイマ回路１２は例えば図６に示すようなフリップフロップを直列に接続したタイマカウンタのようなものでよい。

【００２２】図７はこの発明の第２実施例で使用されるＩＣカードと端末機からなるシステムの機能的構成を示すブロック図である。図２に示す第１実施例のものと異なる点は、ＩＣカード１３にハードウェアとしてのタイマ回路１２が設けられ、端末機２７にも同様のハードウェアとしてのタイマ回路３６が設けられている点、および端末機２７からＩＣカード１３へ送信されるカウント開始信号(ＣＳＳ)が無い点である。また図８および図９には図７のシステムのＩＣカードと端末機との間で行われるこの発明の第２実施例による認証作業(動作)を説明するためのフローチャートを示した。

【００２３】次に図７～図９に従って第２実施例の動作を説明する。上記第１実施例ではソフトウェア上でカウント処理を行っているため、この第２実施例とは目的の認証コード(ＫＥＹ)を断定するための時間情報を得る方法が異なる。この実施例では乱数の送信時にＩＣカード１３と端末機２７の同期をとるようにしている。図８および図９に示すように、ＩＣカード１３より乱数の送信が行われた後(ステップ８３)にＩＣカード１３および端

末機２７でそれぞれタイマ回路１２、３６でカウントを開始する。ここで乱数がＩＣカード１３から送信されるのと、端末機２７で乱数が受信されるのは同時とみなす。これは他の信号或はデータの送受信でも同様であり、また上記第１実施例でも同様である。そして上記乱数が送信された時点から、端末機２７で作られた暗号化された認証データｆ′１(R、S、ＫＥＹ)がＩＣカード１３で受信されるまでの時間をカウントし、この時間から目的の認証コード(ＫＥＹ)を割り出すようにしている(ステップ８７、８８、８９、９０、９１、９２)。その他の処理は第１実施例と同様であり、説明は省略する。

【００２４】上記第１および第２実施例では各認証コード(ＫＥＹ)に対応する時間情報(ＴＩＭＥ)を割り付け、この時間情報をコマンド間或は信号間の時間間隔として送るようにしていたが、複数の暗号化用アルゴリズムを利用して行う方法を以下に説明する。

【００２５】図１０はこの発明の第３実施例で使用されるＩＣカードと端末機からなるシステムの機能的構成を示すブロック図である。図１１には図１０のＩＣカード１３のデータメモリ５内の領域５－ｅおよび端末機２７のデータメモリ２４の領域２４－ｃの内容を示した。そして図１２および図１３には図１０のシステムのＩＣカードと端末機との間で行われるこの発明の第３実施例による認証作業(動作)を説明するためのフローチャートを示した。

【００２６】図１０のＩＣカードと端末機からなるシステムにおいて、上記第１および第２実施例と異なる点は第１に、ＩＣカード１３のデータメモリ５に２つの暗号化用アルゴリズムｆ１、ｇ１および２つのシステムキーＳ１、Ｓ２が格納されており、同様に端末機２７のデータメモリ２４にも２つの暗号化用アルゴリズムｆ′１、ｇ′１および２つのシステムキーＳ１、Ｓ２が格納されている点である。第２にはデータメモリ５、２４の領域５－ｅ、２４－ｃに、図１１に示すテーブルが格納されている点である。このテーブルは各認証コード(ＫＥＹ)にそれぞれ割り当てられた識別子(ＫＩＤ)を示すものである。

【００２７】次に図１０～図１３に従って第３実施例の動作を説明する。ＩＣカード１３より乱数(Ｒ)が送信され(ステップ１２２)、端末機２７でこの乱数(Ｒ)を受信すると(ステップ１３２)、端末機２７では認証の目的の認証コード(ＫＥＹ)を使用して上記実施例と同様に暗号化された認証データｆ′１(R、Ｓ１、ＫＥＹ)を生成し(ステップ１３３)、同時に図１１のテーブルから得られ該認証コード(ＫＥＹ)の識別子(ＫＩＤ)を暗号化してデータｇ′１(ＫＩＤ、Ｓ２)を生成する(ステップ１３４)。そして生成された２つの認証データｆ′１(R、Ｓ１、ＫＥＹ)およびｇ′１(ＫＩＤ、Ｓ２)をＩＣカード１３へ送信する(ステップ１３５)。

【００２８】ＩＣカード１３はこれらの認証データを受

信後(ステップ１２３)、ｇ′１(ＫＩＤ、Ｓ２)を複合化してＫＩＤを求め(ステップ１２４)、このＫＩＤからデータメモリ５に格納されたテーブルにより目的の認証コード(ＫＥＹ)を得る(ステップ１２５)。そしてこの認証コードを使用して暗号化された認証データｆ１(R、Ｓ１、ＫＥＹ)を算出し(ステップ１２６)、端末機２７より送信された認証データｆ′１(R、Ｓ１、ＫＥＹ)と照合を行い(ステップ１２７、１２８、１２９)、一致したか否かを示す結果信号(ＲＴＮ)を端末機２７へ送信する(ステップ１３０)。このようにすれば、外部に直接的な認証コードが格納されているアドレス等を知られることなく認証作業を行うことができる。

【００２９】一般的にＩＣカードはＲＯＭ容量、ＲＡＭ容量、データメモリ等のリソースに制限があり、暗号化アルゴリズム(ｆ′１、ｇ′１)等のプログラムがＩＣカード側に収めることができない場合もある。また、アプリケーションによっては複数の暗号化アルゴリズムを条件によって使い分けする場合もある。このような場合を想定してこの発明の第４実施例では、この問題を解決できるように、例えば認証作業の前に暗号化アルゴリズムを端末機２７からＩＣカード１３へロードするようにした。

【００３０】図１４はこの発明の第４実施例で使用されるＩＣカードと端末機からなるシステムの機能的構成を示すブロック図である。図１０に示された第３実施例のものと異なる点は、ＩＣカード１３のデータメモリ５内に暗号化アルゴリズムｆ１、ｇ１が格納されていない点である。また図１５は図１４のシステムのＩＣカードと端末機との間で行われるこの発明の第４実施例による認証作業(動作)におけるＩＣカードの動作のフローチャートを示した。

【００３１】この実施例では、ＩＣカード１３から乱数(Ｒ)を発生した後(ステップ１４２)、端末機２７側からＩＣカード１３へ暗号化アルゴリズム(ｆ′１)(ｇ′１)を送信し(ステップ１４３)する。ＩＣカード１３ではＲＡＭ３の領域３－ａおよび３－ｂ、もしくはデータメモリ５の空き領域５－ｉおよび５－ｊにこれらの暗号化アルゴリズム(ｆ′１)(ｇ′１)をロードする(ステップ１４４)。そしてその後、上記実施例で行われている認証処理(作業)を行うようにした(ステップ１４５)。なお、認証処理の前に暗号化アルゴリズムを端末機側からＩＣカード側へ送信することは、上記各実施例に適用可能である。

【００３２】また、ＩＣカードと端末機間のトランザクション上のセキュリティを高めるために、トランザクションの回数をカウントし、ある設定値、例えば１００回に達した時に、別の認証コードによる認証を必要とするようにした実施例を以下に示す。

【００３３】図１６～１８はこの発明の第５実施例によるＩＣカードと端末機との間の認証方法を示すフローチ

ャートであり、図１７および図１８は図１６中のそれぞれ送信処理、受信処理を詳しく示している。以下図に従って第５実施例の動作を説明する。

【００３４】この実施例では、ＩＣカードと端末機との間のトランザクションの回数は、例えば第１実施例を示す図２のＩＣカード１３のＣＰＵ１もしくは端末機２７のＣＰＵ２１でトランザクションの回数をインクリメントするなどしてカウントする。そして最初の認証処理（図１６のステップ１５３）が行われる前に、ＣＰＵのトランザクションカウンタをリセットする（ステップ１５２）。その後、様々の処理が行なわれる中でＩＣカード１３と端末機２７との間にデータの送受信が発生する。その送信および受信の回数をカウントしながら認証を行う。

【００３５】図１７は図１６中の送信処理（ステップ１５４）での詳細の動作を示す。送信する前にはトランザクションカウンタを＋１だけインクリメントし（ステップ１６２）、トランザクションの回数が１００回に達したか否かを判断する（ステップ１６３）。１００回に達していれば別の認証コードによる認証処理を行い（ステップ１６４）、認証処理で認証が正しく行われればデータを送信し、その後、トランザクションカウンタをリセットする（ステップ１６７、１６８、１６９）。また１００回に達していなければそのままデータを送信する（ステップ１６５）。

【００３６】一方、受信処理（ステップ１５５）の場合は、図１８に示すようにデータの受信後（ステップ１７２）、トランザクションカウンタを＋１だけインクリメントし（ステップ１７３）、トランザクションの回数が１００回に達したか否か判定する（ステップ１７４）。１００回に達していれば別の認証コードで認証処理を行い（ステップ１７５）、その後、トランザクションカウンタをリセットする（ステップ１７６）。また１００回に達していなければそのまま次の処理に移行する。

【００３７】また、複数の認証コード（ＫＥＹ）を持つ場合に、認証に使用する認証コードをランダムに選択する方法を付加することにより、より一層セキュリティの高いものが実現できる。図１９には乱数を利用して認証コードをランダムに選択する機能を付加した、この発明の第６実施例による認証方法の動作を示すフローチャートが示されている。以下、この動作について説明する。

【００３８】例えば認証コード（ＫＥＹ）（Ａ、Ｂ、Ｃ…）の数がＮ個である場合には、乱数（Ｒ）を認証コード（ＫＥＹ）の個数Ｎ個で割り、残りｍを求め（ステップ１８３）、ｍ＋１番目の認証コード（ＫＥＹ）を選択することにより（ステップ１８４～１８９）、ランダムに認証コードを選択することができる。例えば、ｍ＝０なら１番目の認証コード（Ａ）、ｍ＝１なら２番目の認証コード（Ｂ）という様に選択する。

【００３９】なお上記各実施例の説明において、ＩＣカード側および端末機側のいずれかを限定して説明した事項は、ＩＣカード側および端末機側の限定を逆にしても同様の認証を行うことができる。例えば乱数発生はＩＣカード側で行っているが、端末機側で行ってもよい。また、上記実施例ではＩＣカードと端末機との間の認証方法について説明したが、この発明は認証を必要とする２つの装置間であれば、どの様な形態でも適用可能である（例えば、端末機と端末機間、システムとシステム間）。

【００４０】

【発明の効果】以上説明したように、この発明によれば、ＩＣカードと端末機との間で、認証コード或は認証コードが記憶されているアドレスを直接伝送することなく認証作業を行うようにしたので、不正使用者に認証コードの内容やアドレスを知られることがなく、セキュリティの非常に高い認証方法およびそのシステムが得られる効果がある。

【図面の簡単な説明】

【図１】この発明で使用されるＩＣカードの機能的構成を一例を示すブロック図である。

【図２】この発明の第１実施例によるＩＣカードと端末機からなるシステムの機能的構成を示すブロック図である。

【図３】図２のＩＣカードおよび端末機のデータメモリ内に格納された認証コードと対応する時間情報の内容を拡大して示した図である。

【図４】この発明の第１実施例による認証方法におけるＩＣカードの動作を示すフローチャート図である。

【図５】この発明の第１実施例による認証方法における端末機の動作を示すフローチャート図である。

【図６】タイマ回路の一例を示す図である。

【図７】この発明の第２実施例によるＩＣカードと端末機からなるシステムの機能的構成を示すブロック図である。

【図８】この発明の第２実施例による認証方法におけるＩＣカードの動作を示すフローチャート図である。

【図９】この発明の第２実施例による認証方法における端末機の動作を示すフローチャート図である。

【図１０】この発明の第３実施例によるＩＣカードと端末機からなるシステムの機能的構成を示すブロック図である。

【図１１】図１０のＩＣカードおよび端末機のデータメモリに格納された認証コードと対応する時間情報の内容を拡大して示した図である。

【図１２】この発明の第３実施例による認証方法におけるＩＣカードの動作を示すフローチャート図である。

【図１３】この発明の第３実施例による認証方法における端末機の動作を示すフローチャート図である。

【図１４】この発明の第４実施例によるＩＣカードと端末機からなるシステムの機能的構成を示すブロック図である。

１５

【図１５】この発明の第４実施例による認証方法におけるＩＣカードの動作を示すフローチャート図である。

【図１６】この発明の第４実施例によるＩＣカードと端末機との間の認証方法を示すフローチャートである。

【図１７】図１６中の送信処理の詳細な動作を示すフローチャートである。

【図１８】図１６中の受信処理の詳細な動作を示すフローチャートである。

【図１９】この発明の第６実施例による認証方法における動作を示すフローチャート図である。

【符号の説明】

１　ＣＰＵ

１６

２　ＵＡＲＴ（入出力制御回路）

３　ＲＡＭ

４　ＲＯＭ

５　データメモリ

６　バス

１３　ＩＣカード

２１　ＣＰＵ

２２　ＲＯＭ

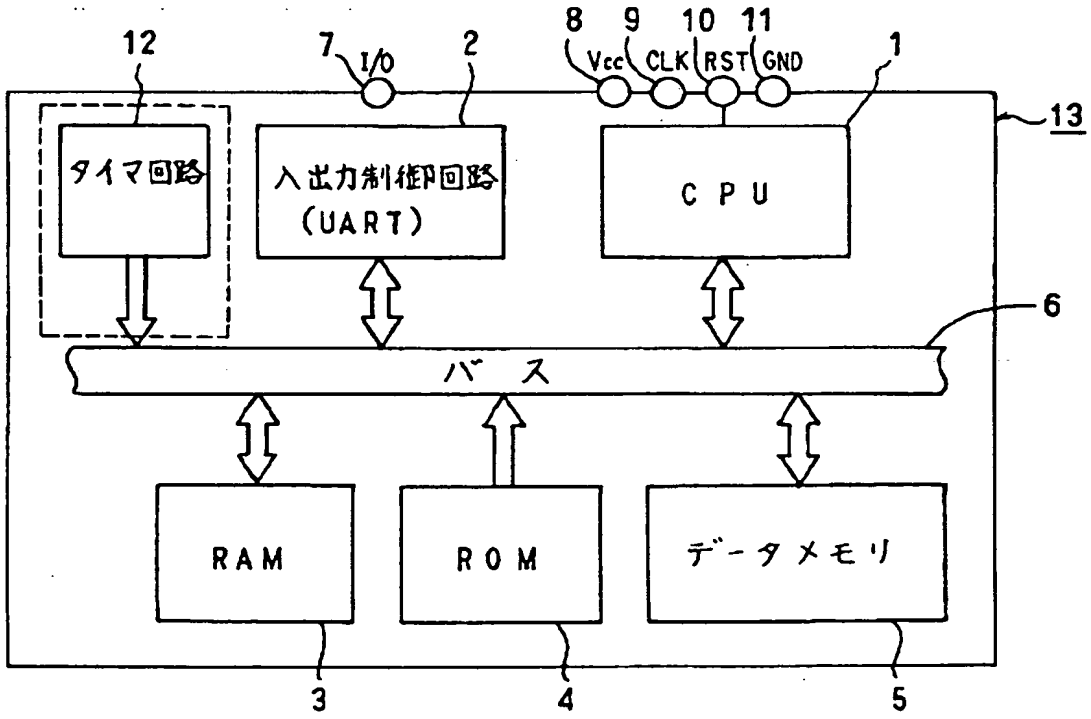
２３　Ｉ／Ｏ

２４　データメモリ

２６　Ｉ／Ｏ

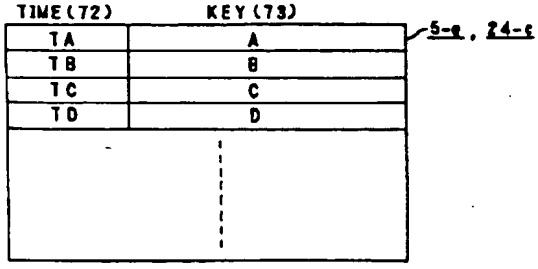
２７　端末機

【図１】

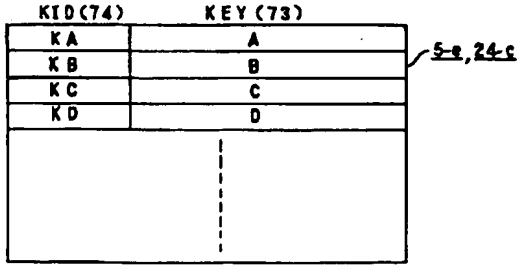


13：ＩＣカード

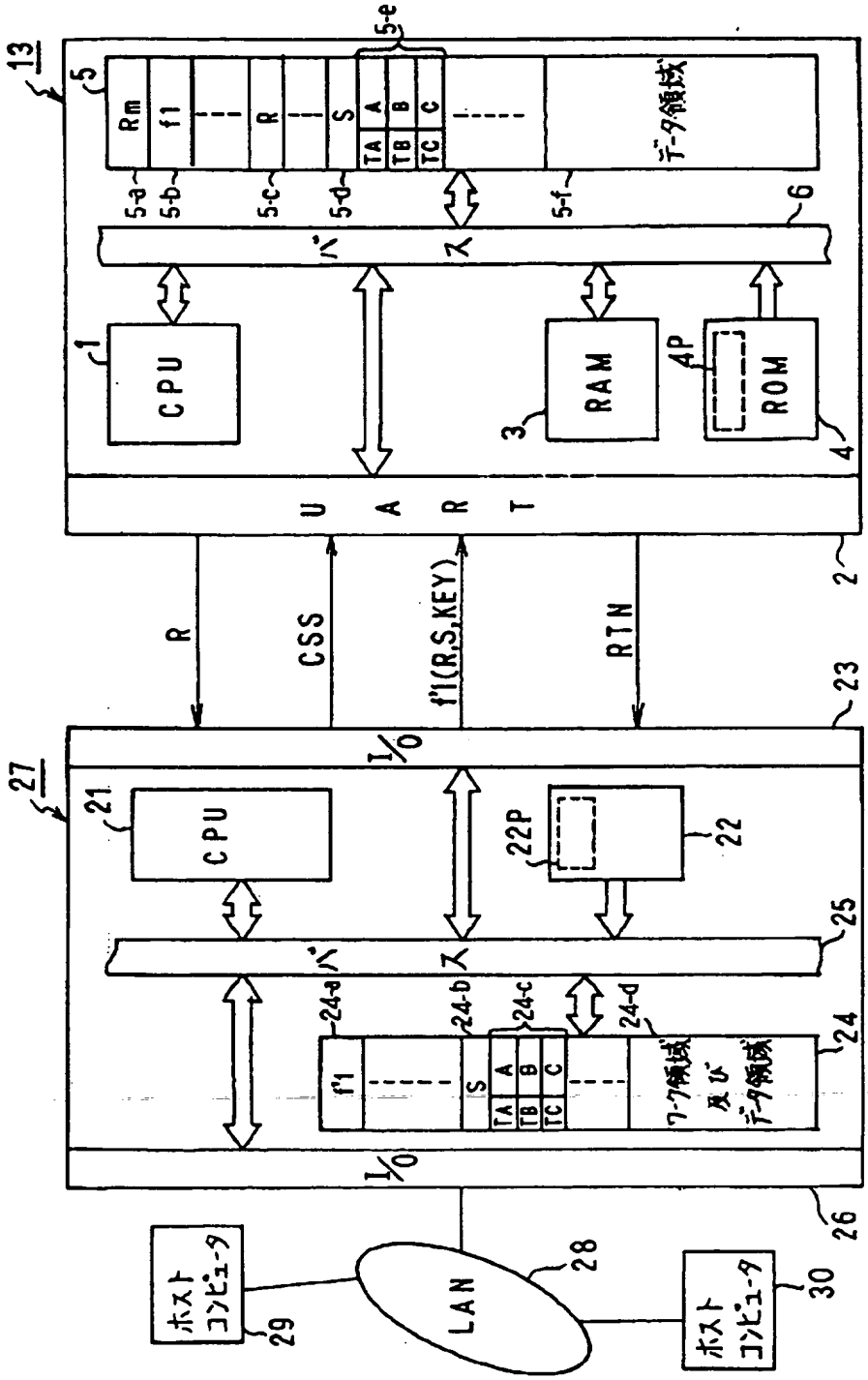
【図３】



【図１１】

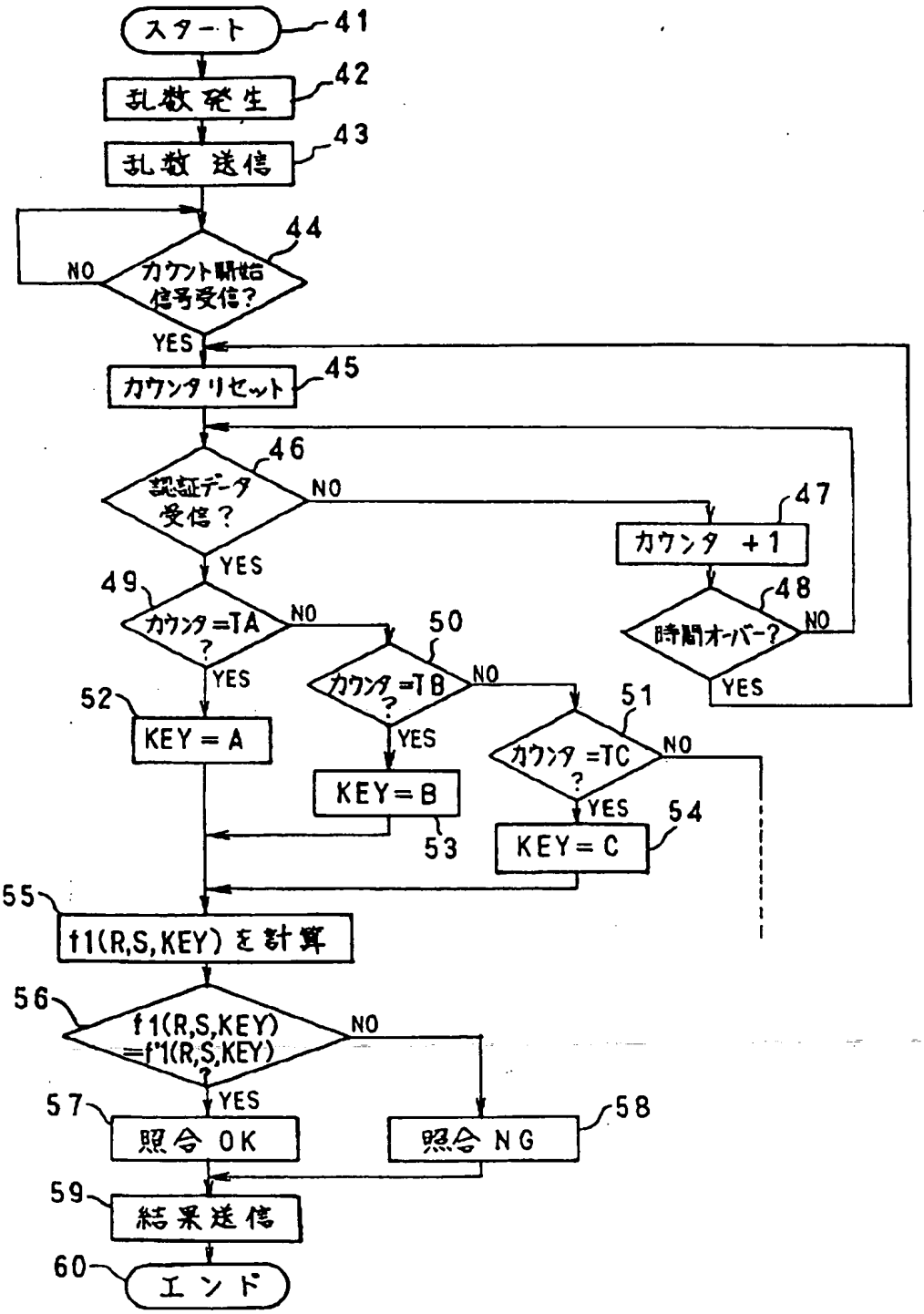


【図2】

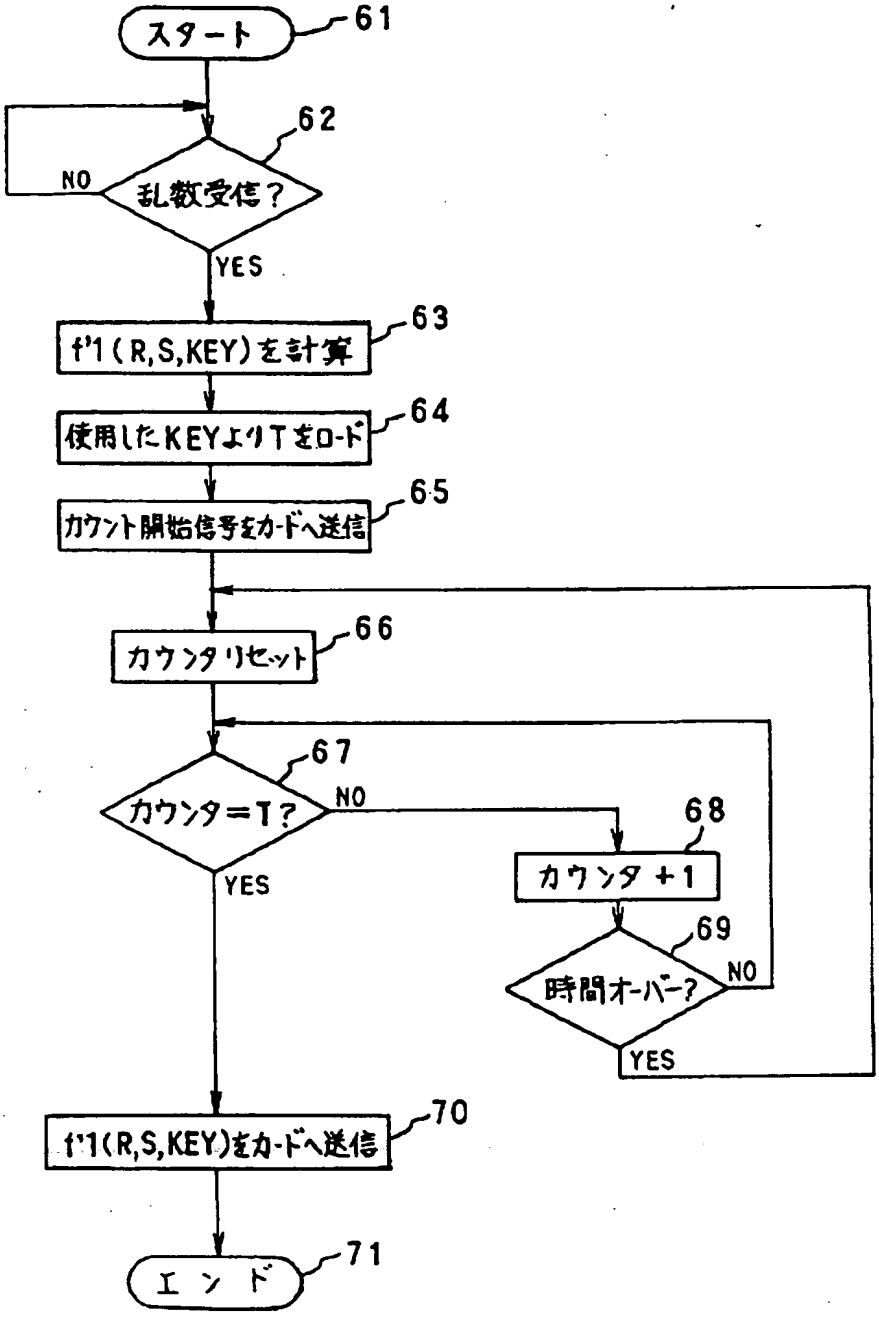


4P, 22P：認証プログラム　13：ICカード
5，24：データメモリ　27：端末機

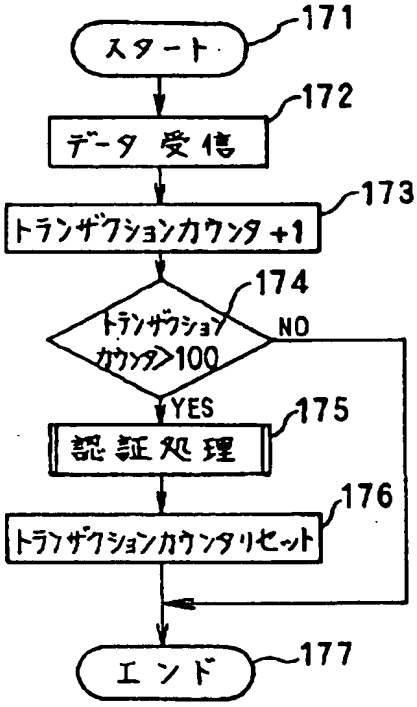
【図4】


スタート
41
乱数発生
42
乱数送信
43
44
NO
カウント開始信号受信?
YES
カウンタリセット
45
46
認証データ受信?
NO
47
カウンタ +1
YES
49
カウンタ=TA?
NO
50
48
時間オーバー?
NO
YES
YES
52
KEY=A
カウンタ=TB?
NO
YES
51
カウンタ=TC?
NO
KEY=B
53
YES
54
KEY=C
55
f1(R,S,KEY)を計算
56
f1(R,S,KEY)=f'1(R,S,KEY)?
NO
YES
57
照合OK
照合NG
58
59
結果送信
60
エンド

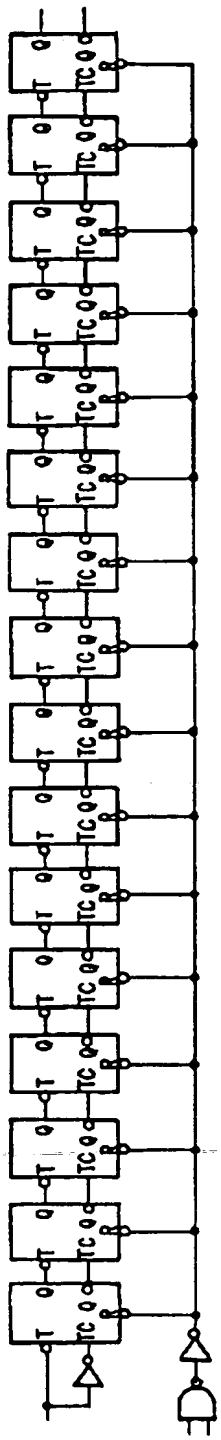
【図５】


スタート
61
62
NO
乱数受信？
YES
f'1(R,S,KEY)を計算
63
使用したKEYよりTをロード
64
カウント開始信号をカードへ送信
65
カウンタリセット
66
67
カウンタ＝T？
NO
YES
68
カウンタ＋1
69
時間オーバー？
NO
YES
f'1(R,S,KEY)をカードへ送信
70
エンド
71

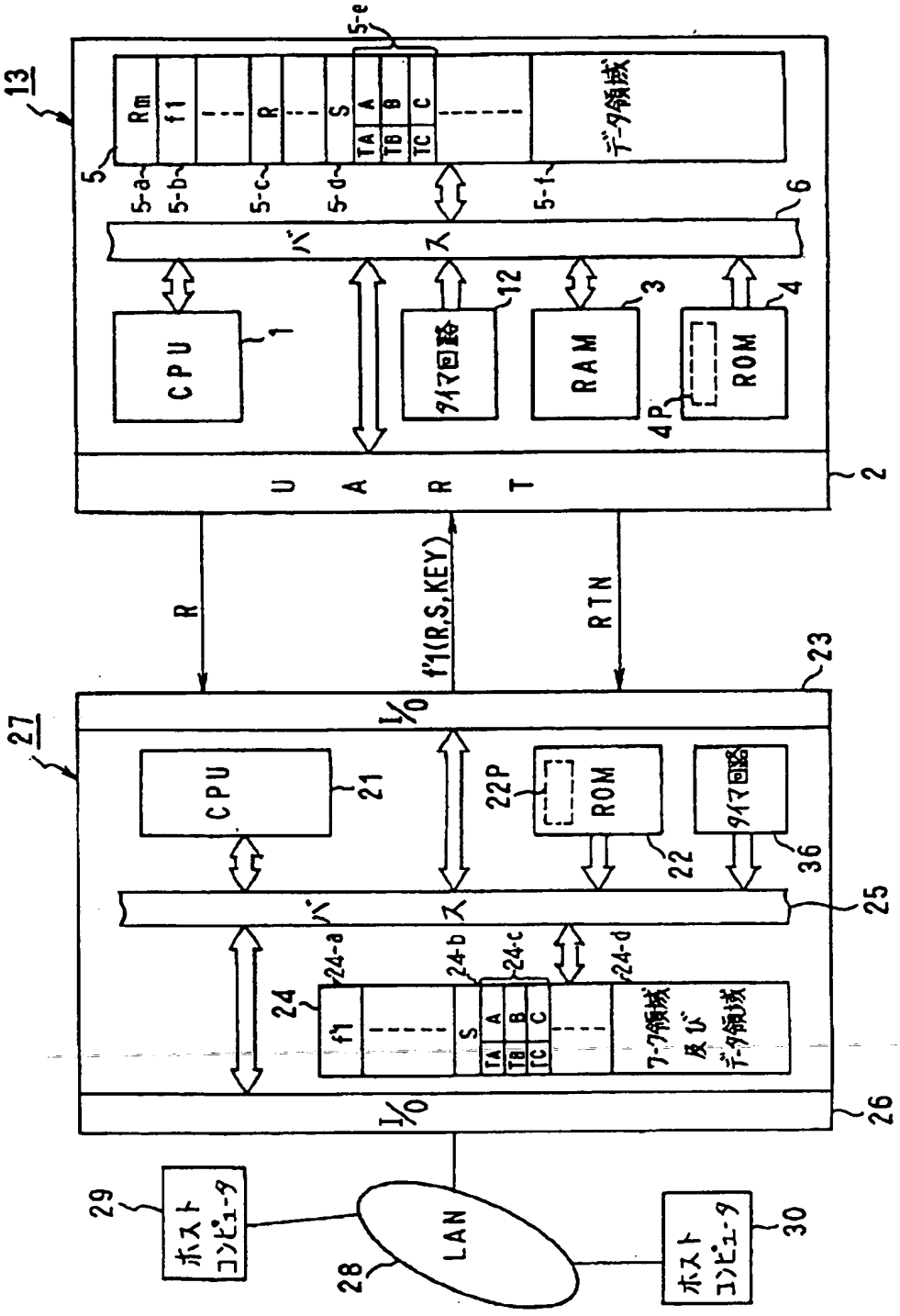
【図１８】


スタート
171
データ受信
172
トランザクションカウンタ+1
173
174
トランザクションカウンタ>100
NO
YES
認証処理
175
トランザクションカウンタリセット
176
エンド
177

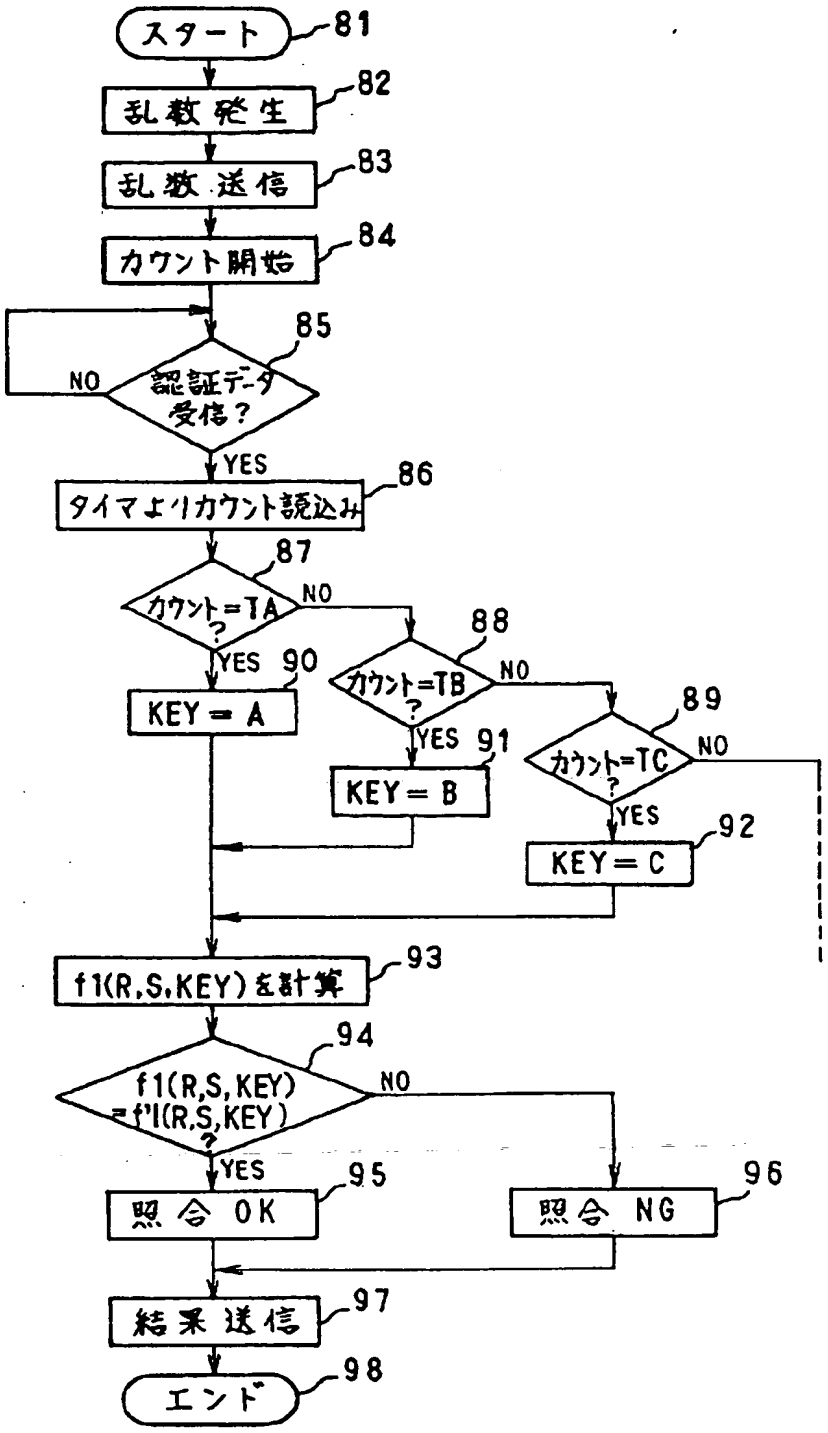
【図６】



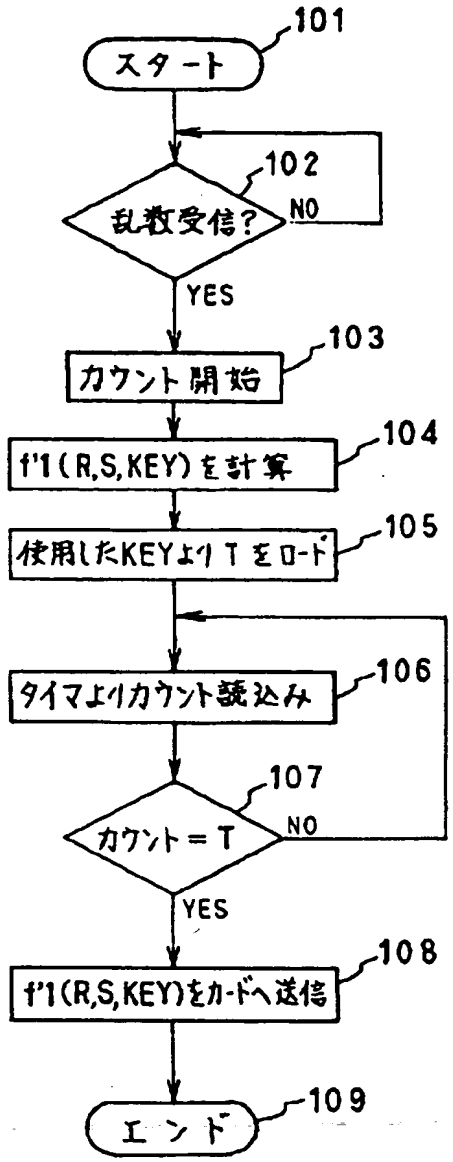
【図7】


13
5
Rm
f1
R
S
TA
TB
TC
A
B
C
データ領域
5-a
5-b
5-c
5-d
5-e
5-f
6
バス
CPU
1
割込回路
12
RAM
3
ROM
4
4P
UART
2
R
f1(R,S,KEY)
RTN
23
I/O
27
CPU
21
22P
ROM
22
割込回路
36
25
24
24-a
24-b
24-c
24-d
f1
S
TA
TB
TC
A
B
C
データ領域及びデータ領域
I/O
26
29
ホストコンピュータ
LAN
28
ホストコンピュータ
30

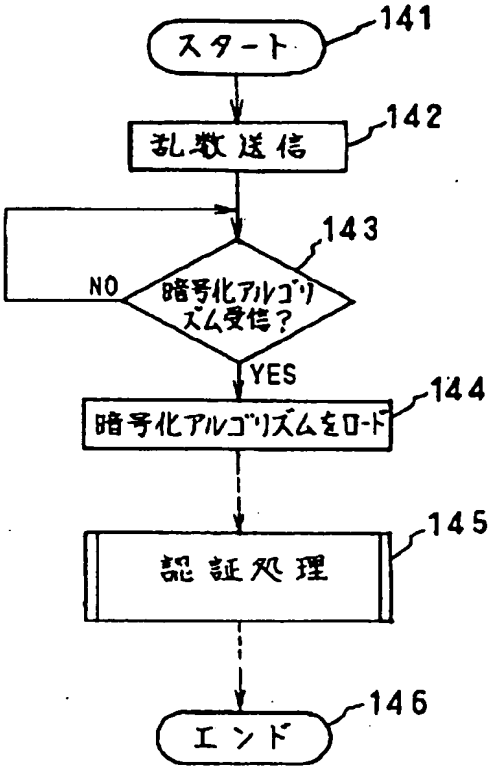
【図8】


スタート
81
乱数発生
82
乱数送信
83
カウント開始
84
85
認証データ受信？
NO
YES
タイマよりカウント読込み
86
87
カウント=TA？
NO
YES
90
KEY＝A
88
カウント=TB？
NO
YES
91
KEY＝B
89
カウント=TC？
NO
YES
92
KEY＝C
f1(R,S,KEY)を計算
93
94
f1(R,S,KEY)=f'1(R,S,KEY)？
NO
YES
照合 OK
95
照合 NG
96
結果送信
97
エンド
98

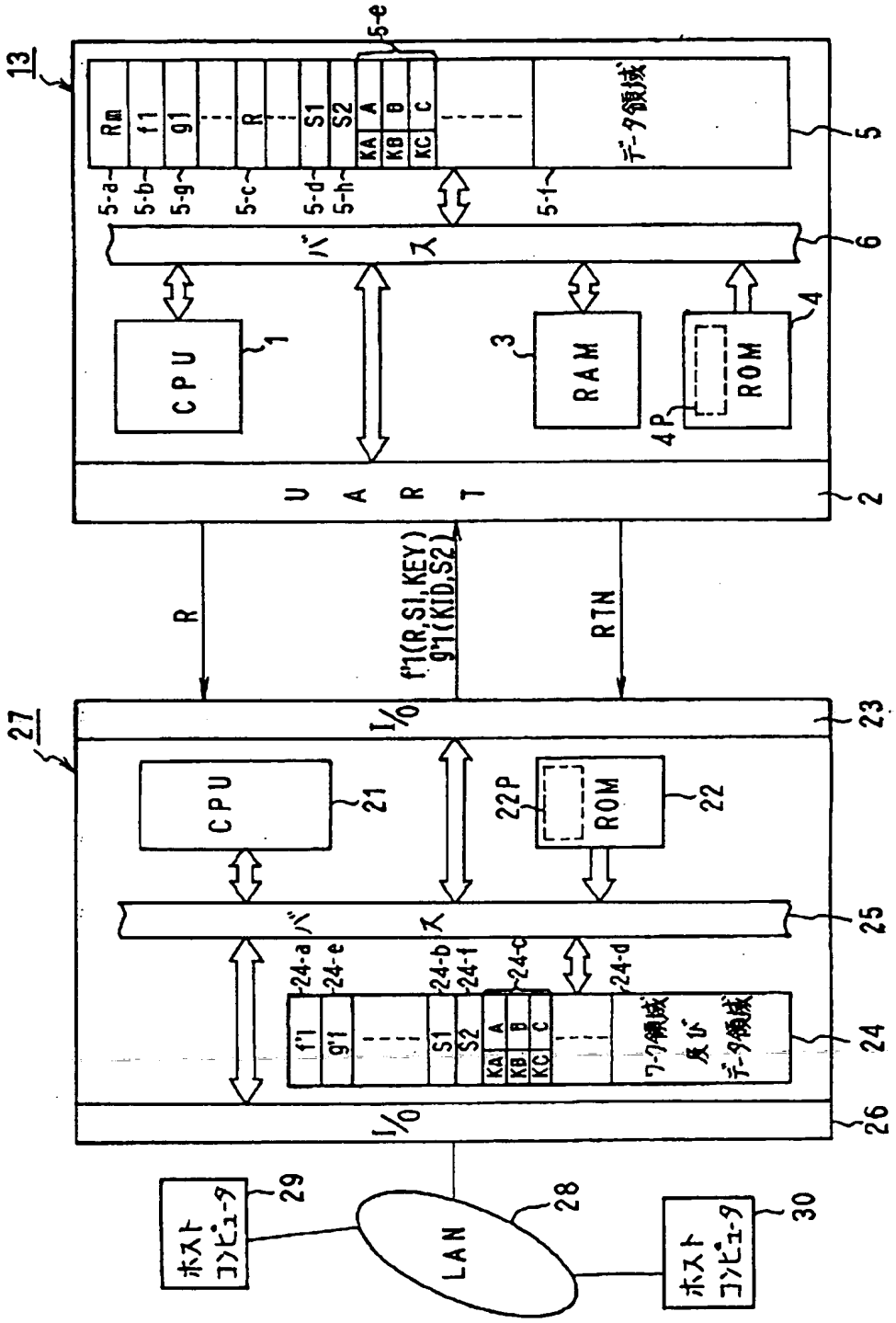
【図9】


101
スタート
102
乱数受信?
NO
YES
103
カウント開始
104
f'1(R,S,KEY)を計算
105
使用したKEYよりTをロード
106
タイマよりカウント読込み
107
カウント=T
NO
YES
108
f'1(R,S,KEY)をカードへ送信
109
エンド

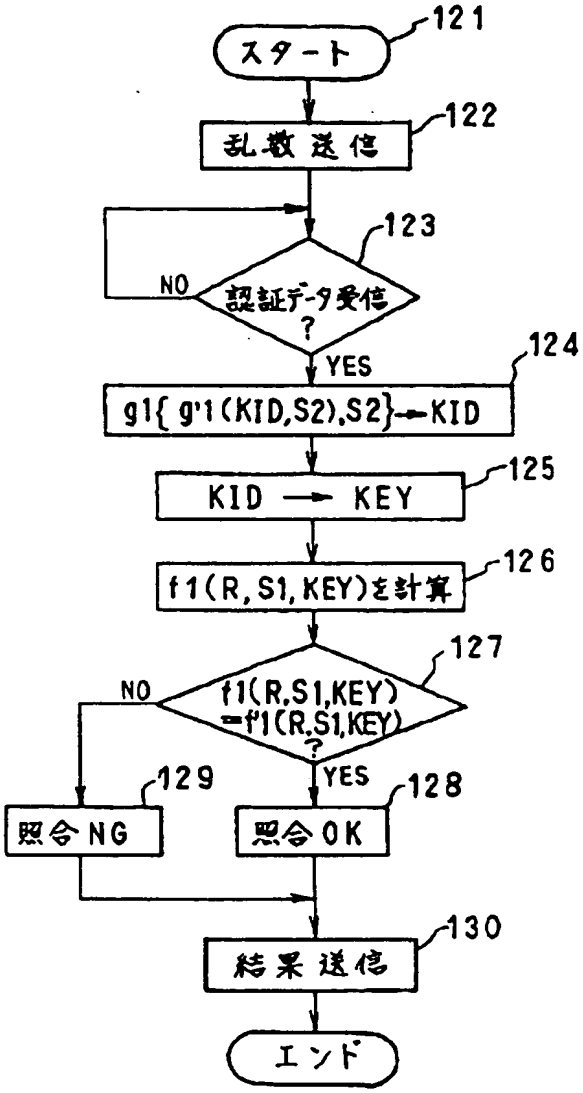
【図15】


141
スタート
142
乱数送信
143
暗号化アルゴリズム受信?
NO
YES
144
暗号化アルゴリズムをロード
145
認証処理
146
エンド

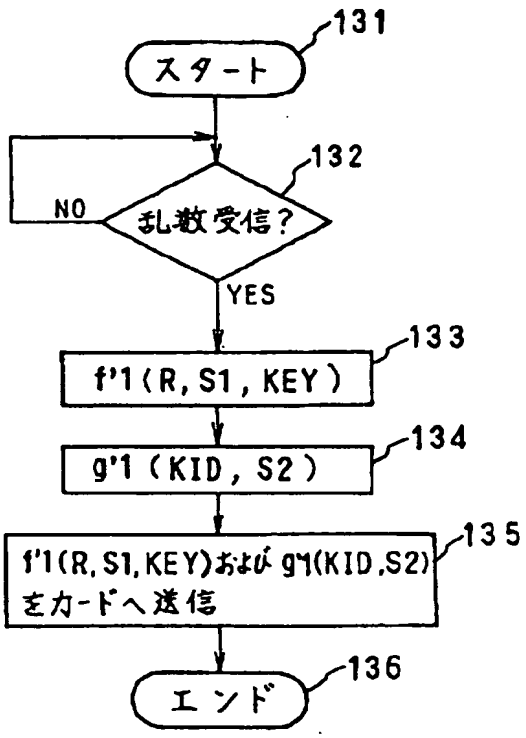
【図10】


13
5-e
Rm
f1
g1
R
S1
S2
A
B
C
KA
KB
KC
データ領域
5
5-a
5-b
5-g
5-c
5-d
5-h
5-f
バス
6
CPU
1
3
RAM
4
4P
ROM
UART
2
R
f'1(R,S1,KEY)
g'1(KID,S2)
RTN
27
I/O
23
CPU
21
22P
ROM
22
バス
25
24-a
24-e
24-b
24-f
24-c
24-d
f'1
g'1
S1
S2
KA
KB
KC
データ領域
データ領域
反転
24
I/O
26
ホストコンピュータ
29
LAN
28
ホストコンピュータ
30

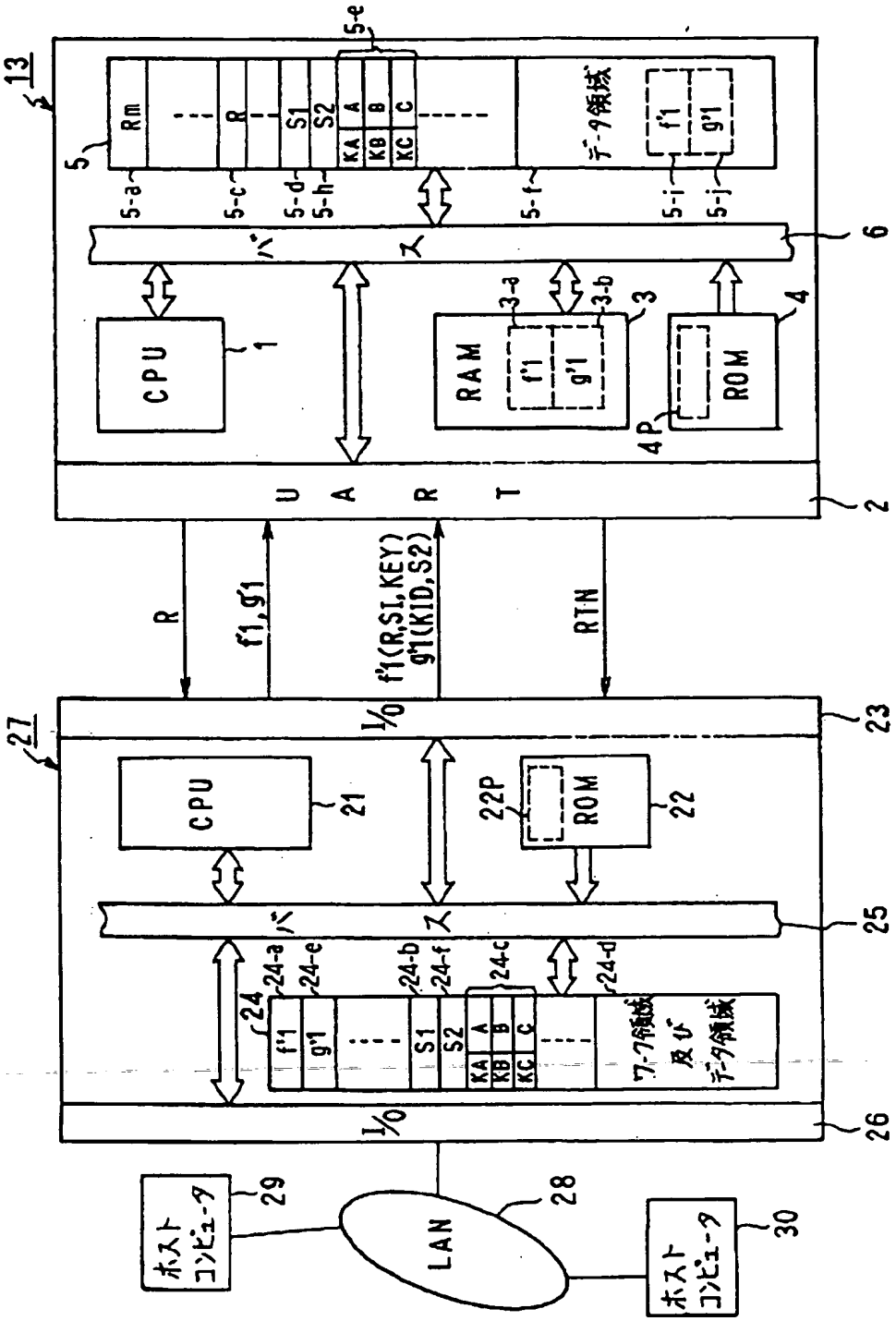
【図１２】


121
スタート
122
乱数送信
123
NO
認証データ受信
?
YES
124
g1{g'1(KID,S2),S2}→KID
125
KID → KEY
126
f1(R,S1,KEY)を計算
127
NO
f1(R,S1,KEY)
=f'1(R,S1,KEY)
?
YES
129
照合NG
128
照合OK
130
結果送信
エンド

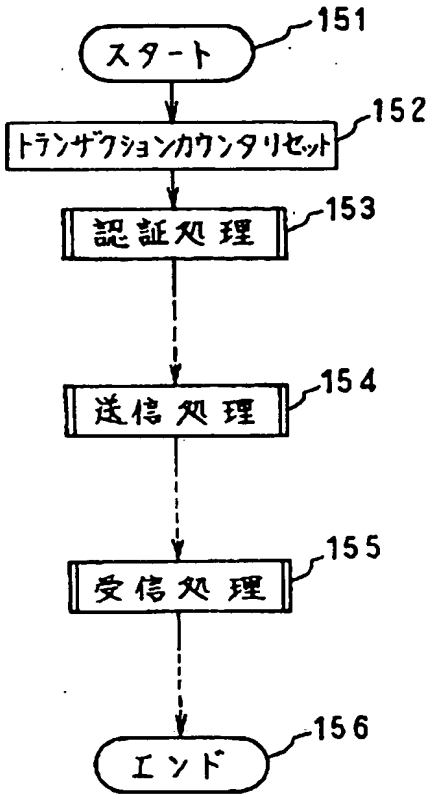
【図１３】


131
スタート
132
NO
乱数受信？
YES
133
f'1(R, S1, KEY)
134
g'1(KID, S2)
135
f'1(R, S1, KEY)およびg'1(KID, S2)
をカードへ送信
136
エンド

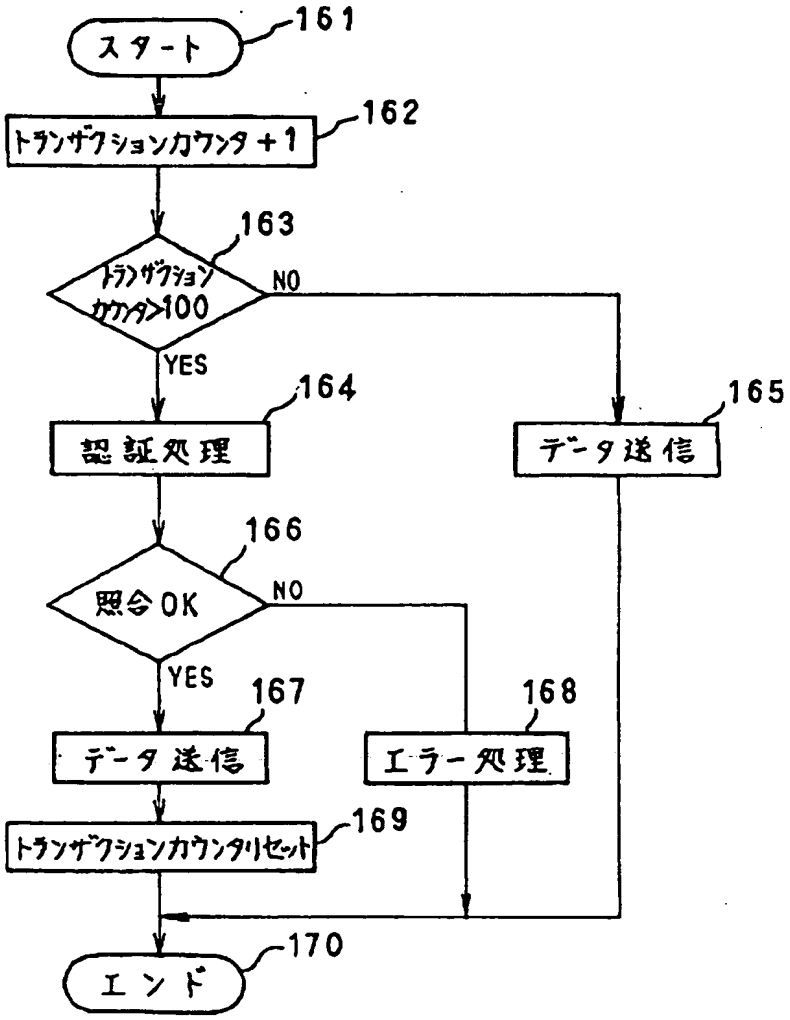
【図１４】


13
5
Rm
R
S1
S2
A
B
C
KA
KB
KC
データ領域
f'1
g'1
5-a
5-c
5-d
5-h
5-e
5-f
5-i
5-j
バス
6
CPU
1
RAM
3
3-a
3-b
ROM
4
4P
UART
2
R
f'1,g'1
f'1(R,SI,KEY)
g'1(KID,S2)
RTN
I/O
23
27
CPU
21
22P
ROM
22
バス
25
24
24-a
24-e
24-b
24-f
24-c
24-d
アドレス及びデータ領域
I/O
26
ホストコンピュータ
29
LAN
28
ホストコンピュータ
30

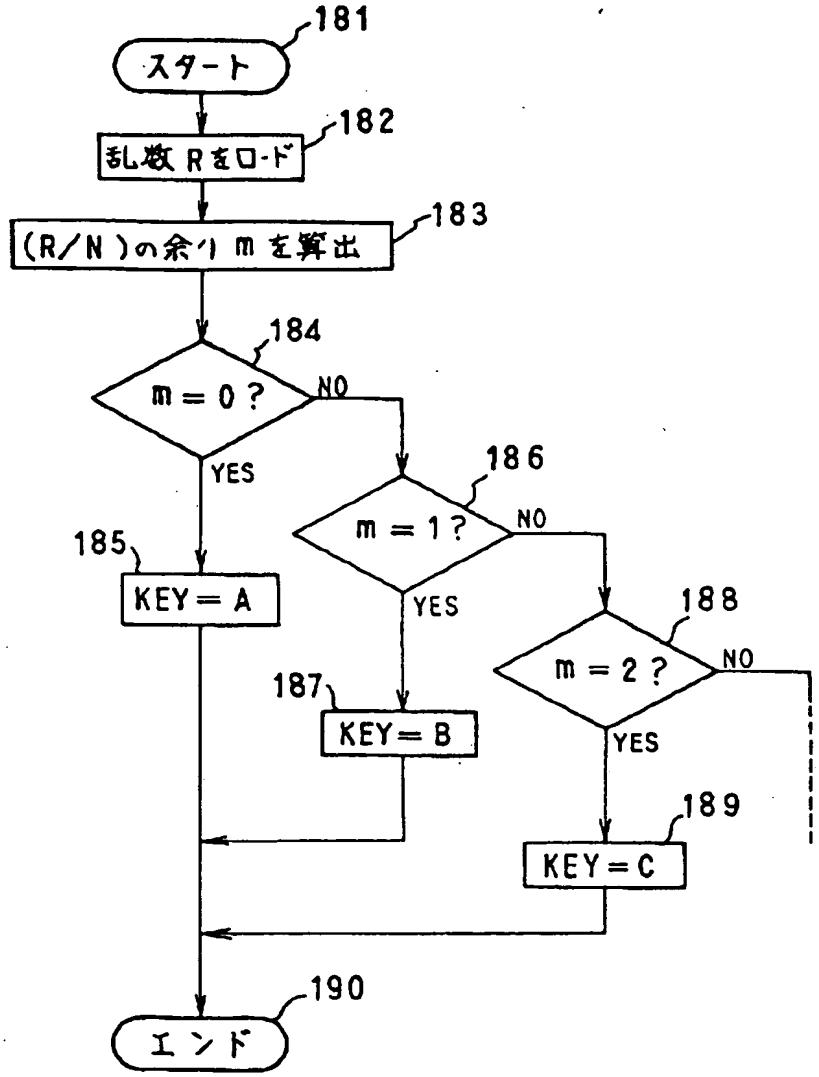
【図１６】


151
スタート
152
トランザクションカウンタリセット
153
認証処理
154
送信処理
155
受信処理
156
エンド

【図１７】


スタート
161
トランザクションカウンタ＋1
162
トランザクション カウンタ>100
163
NO
YES
認証処理
164
データ送信
165
照合OK
166
NO
YES
データ送信
167
エラー処理
168
トランザクションカウンタリセット
169
エンド
170

【図１９】



【手続補正書】
【提出日】平成５年４月９日
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】００３１
【補正方法】変更
【補正内容】
【００３１】この実施例では、ＩＣカード１３から乱数(R)を発生した後(ステップ１４２)、端末機２７側からＩＣカード１３へ暗号化アルゴリズム(f′1)(g′1)を送信する(ステップ１４３)。ＩＣカード１３ではＲＡＭ３の領域３－ａおよび３－ｂ、もしくはデータメモリ５の空き領域５－ｉおよび５－ｊにこれらの暗号化アルゴリズム(f′1)(g′1)をロードする(ステップ１４４)。そしてその後、上記実施例で行われている認証処理(作業)を行うようにした(ステップ１４５)。なお、認証処理の前に暗号化アルゴリズムを端末機側からＩＣカード側へ送信することは、上記各実施例に適用可能である。